

KAPLAN FOX & KILSHEIMER LLP

Laurence D. King (SBN 206423)
Matthew B. George (SBN 239322)
Blair E. Reed (SBN 316791)
1999 Harrison Street, Suite 1560
Oakland, CA 94612
Telephone: 415-772-4700
Facsimile: 415-772-4707
Email: *lking@kaplanfox.com*
mgeorge@kaplanfox.com
breed@kaplanfox.com

**KANTROWITZ, GOLDHAMER
& GRAIFMAN P.C.**

Melissa R. Emert (admitted *pro hac vice*)
Gary S. Graifman (admitted *pro hac vice*)
135 Chestnut Ridge Road, Suite 200
Montvale, NJ 07645
Telephone: 201-391-7000
Facsimile: 302-307-1086
Email: *memert@kgglaw.com*
ggraifman@kgglaw.com

Interim Co-Lead Class Counsel

Attorneys for Plaintiffs

[Additional Counsel Appear on Signature Page]

**UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA**

*In re: Illuminate Education Data
Security Incident Litigation*

Case No. 8:22-cv-1164-JVS-ADSx

**PLAINTIFFS' MEMORANDUM OF POINTS AND AUTHORITIES IN
OPPOSITION TO DEFENDANT ILLUMINATE EDUCATION, INC.'S
MOTION TO DISMISS THE CONSOLIDATED COMPLAINT**

TABLE OF CONTENTS

	Page
1 INTRODUCTION.....	1
2 FACTUAL BACKGROUND	1
3 ARGUMENT	4
4 I. PLAINTIFFS HAVE ADEQUATELY ALLEGED ARTICLE	
5 III STANDING	4
6 A. Plaintiffs Pleaded Concrete Injuries	4
7 1. An Increased Risk of Harm from Identify Theft.....	4
8 a. Illuminate's Notification Letter to Plaintiffs	
9 Concede Their Risk of Future Harm.....	8
10 2. Plaintiffs' Allegations of Diminished Value of	
11 Their PI/PHI is a Concrete Injury	8
12 3. Plaintiffs' Loss of Time and/or Money Expended to	
13 Mitigate the Risk of Harm Confers Standing.....	9
14 4. Plaintiffs Have Been Further Injured by	
15 Illuminate's Delay	9
16 II. CHOICE OF LAW	9
17 III. PLAINTIFFS HAVE ADEQUATELY PLEADED CAUSES	
18 OF ACTION FOR NEGLIGENCE	10
19 A. Illuminate Was Negligent, As Evidenced By The Data	
20 Breach.....	10
21 B. The Economic Loss Doctrine Does Not Preclude	
22 Plaintiffs' Negligence Claims.....	12
23 C. Negligence <i>Per Se</i> Has Been Plausibility Pleaded	13
24 IV. PLAINTIFFS STATE A CLAIM FOR BREACH OF	
25 CONTRACT	14
26 V. PLAINTIFFS STATE A CLAIM FOR INVASION OF	
27 PRIVACY	17
28 VI. PLAINTIFFS ADEQUATELY ALLEGE THEIR BREACH OF	
CONFIDENCE CLAIM	19
VII. PLAINTIFFS' STATUTORY CLAIMS ARE ADEQUATELY	
PLEADED	21
A. Plaintiffs Are Not Required To Prove Reliance Under The	
Statutory Claims Alleged	21

TABLE OF CONTENTS (cont'd.)

	Page
B. Plaintiffs Have Adequately Pleaded Their California Consumer Privacy Act (“CCPA”) and California Confidentiality of Medical Information Act (“CMIA”) Claims	24
1. CCPA	24
2. CMIA	25
C. Plaintiffs Have A Right Of Action Under The Colorado Security Breach Notification Act	27
VIII. PLAINTIFFS’ REQUEST FOR DECLARATORY RELIEF IS NOT DUPLICATIVE.....	27
CONCLUSION	28

TABLE OF AUTHORITIES

Page(s)

1 CASES

2	<i>Berkson v. Gogo LLC,</i>	
3	87 F. Supp. 3d 359 (E.D.N.Y. 2015)	16
4	<i>Castillo v. Seagate Tech., LLC,</i>	
5	2016 WL 9280242 (N.D. Cal. Sept. 14, 2016)	17
6	<i>Clancy v. The Bromley Tea Co.,</i>	
7	308 F.R.D. 564 (N.D. Cal. 2013)	10
8	<i>Clemens v. ExecuPharm Inc.,</i>	
9	48 F. 4th 146 (3d Cir. 2022)	5, 6
10	<i>Cnty. Bank of Trenton v. Schnuck Markets, Inc.,</i>	
11	887 F.3d 803 (7th Cir. 2018)	11
12	<i>Cohen v. Ne. Radiology, P.C.,</i>	
13	2021 WL 293123 (S.D.N.Y. Jan. 28, 2021)	16
14	<i>Corona v. Sony Pictures Ent., Inc.,</i>	
15	2015 WL 3916744 (C.D. Cal. June 15, 2015)	26
16	<i>Cummings v. Entergy Int'l Servs., LC,</i>	
17	271 F. Supp. 3d 1182 (E.D. Cal. 2017)	17
18	<i>Dugas v. Starwood Hotels & Resorts Worldwide, Inc.,</i>	
19	2016 WL 6523428 (S.D. Cal. Nov. 3, 2016)	18
20	<i>Ehret v. Uber Techs., Inc.,</i>	
21	68 F.Supp.3d 1121 (N.D. Cal. 2014)	10
22	<i>Engl v. Nat. Grocers by Vitamin Cottage, Inc.,</i>	
23	2016 WL 8578096 (D. Colo. June 20, 2016)	27
24	<i>Ent. Rsch. Grp., Inc. v. Genesis Creative Grp., Inc.,</i>	
25	122 F.3d 1211 (9th Cir. 1997)	19, 20
26	<i>Fairfield v. American Photocopy etc. Co.,</i>	
27	138 Cal. App. 2d 82 (Cal. Ct. App. 1955)	18
28	<i>Feldman v. CSX Transp., Inc.,</i>	
	31 A.D.3d 698, 821 N.Y.S.2d 85 (2d Dep't 2006)	14
	<i>Gaston v. FabFitFun, Inc.,</i>	
	2021 WL 3362028 (C.D. Cal. Apr. 2, 2021)	23
	<i>Gordon v. Chipotle Mexican Grill, Inc.,</i>	
	344 F. Supp. 3d 1231 (D. Colo. 2018)	16
	<i>Griffey v. Magellan Health Inc.,</i>	
	2022 WL 1811165 (D. Ariz. June 2, 2022)	23
	<i>Grimstad v. FCA US, LLC,</i>	
	2018 WL 6265087 (C.D. Cal. May 24, 2018)	22

TABLE OF AUTHORITIES (cont'd.)**Page(s)**

1	<i>Hameed-Bolden v. Forever 21 Retail, Inc.</i> ,	
2	2018 WL 6802818 (C.D. Cal. Oct. 1, 2018).....	16
3	<i>Hill v. NCAA</i> ,	
4	7 Cal. 4th 1 (1994)	18, 19
5	<i>Huynh v. Quora, Inc.</i> ,	
6	508 F. Supp. 3d 633 (N.D. Cal. 2020)	13, 21
7	<i>I.C. v. Zynga, Inc.</i> ,	
8	2022 WL 2252636 (N.D. Cal. Apr. 29, 2022)	7, 8
9	<i>In re Adobe Sys., Inc. Priv. Litig.</i> ,	
10	66 F. Supp. 3d 1197 (N.D. Cal. 2014)	22
11	<i>In re Ambry Genetics Data Breach Litig.</i> ,	
12	567 F. Supp. 3d 1130 (C.D. Cal. 2021)	14, 19
13	<i>In re Anthem, Inc. Data Breach Litig.</i> ,	
14	2016 WL 3029783 (N.D. Cal. May 27, 2016)	9
15	<i>In re Blackbaud, Inc. Customer Data Breach Litig.</i> ,	
16	2021 WL 2718439 (D.S.C. July 1, 2021)	6
17	<i>In re Blackbaud, Inc., Customer Data Breach Litig.</i> ,	
18	2021 WL 3568394 (D.S.C. Aug. 12, 2021)	23, 24, 25, 26
19	<i>In re Cap. One Consumer Data Sec. Breach Litig.</i> ,	
20	488 F. Supp. 3d 374 (E.D. Va. 2020)	21
21	<i>In re Clorox Consumer Litig.</i> ,	
22	894 F. Supp. 2d 1224 (N.D. Cal. 2012)	10
23	<i>In re Equifax, Inc., Customer Data Sec. Breach Litig.</i> ,	
24	362 F. Supp. 3d 1295 (N.D. Ga. 2019)	27
25	<i>In re Facebook Internet Tracking Litig.</i> ,	
26	956 F.3d 589 (9th Cir. 2020)	18
27	<i>In re iPhone 4S Consumer Litig.</i> ,	
28	2013 WL 3829653 (N.D. Cal. July 23, 2013)	10
	<i>In re iPhone Application Litig.</i> ,	
	844 F. Supp. 2d 1040 (N.D. Cal. 2012)	18
	<i>In re Premiera Blue Cross Customer Data Security Breach Litig.</i> ,	
	2017 WL 539578 (D. Ore. Feb. 9, 2017)	15
	<i>In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.</i> ,	
	2020 WL 2214152 (S.D. Cal. May 7, 2020)	12, 26, 27
	<i>In re Sony Gaming Networks & Customer Data Sec. Breach Litig.</i> ,	
	903 F.Supp.2d 942 (S.D. Cal. 2012)	12

TABLE OF AUTHORITIES (cont'd.)**Page(s)**

1	<i>In re Waste Mgmt. Data Breach Litig.</i> ,	
2	2022 WL 561734 (S.D.N.Y. Feb. 24, 2022).....	11
3	<i>In re Yahoo! Inc. Customer Data Security Breach Litig.</i> ,	
4	2017 WL 3727318 (N.D. Cal. Aug. 30, 2017)	8, 16
5	<i>In re Zappos.com, Inc. Customer Data Security Breach Litig.</i> ,	
6	888 F.3d 1020 (9th Cir. 2018)	5
7	<i>Kalitta Air, L.L.C. v. Cent. Texas Airborne Sys., Inc.</i> ,	
8	315 F. App'x 603 (9th Cir. 2008)	12
9	<i>Karter v. Epiq Sys., Inc.</i> ,	
10	2021 WL 4353274 (C.D. Cal. July 16, 2021).....	24, 25
11	<i>Krottner v. Starbucks Corp.</i> ,	
12	628 F.3d 1139 (9th Cir. 2010)	5
13	<i>Lugo v St. Nicholas Assoc.</i> ,	
14	2 Misc. 3d 212, 772 N.Y.S.2d 449 (N.Y. Sup. Ct. 2003)	14
15	<i>Mangindin v. Wash. Mut. Bank</i> ,	
16	637 F. Supp. 2d 700 (N.D. Cal. 2009)	28
17	<i>McKenzie v. Allconnect, Inc.</i> ,	
18	369 F. Supp. 3d 810 (E.D. Ky. 2019)	6
19	<i>Morrison v. Ross Stores</i> ,	
20	2019 WL 11770849 (N.D. Cal. May 30, 2019).....	10
21	<i>Patton v. Experian Data Corp.</i> ,	
22	2018 WL 6190349 (C.D. Cal. Jan. 23, 2018)	24
23	<i>Pauwels v. Deloitte LLP</i> ,	
24	2020 WL 818742 (S.D.N.Y. Feb. 19, 2020).....	20
25	<i>Pelman ex rel. Pelman v. McDonald's Corp.</i> ,	
26	396 F.3d 508 (2d Cir. 2005)	23
27	<i>Robert C Ozer, P.C. v. Borquez</i> ,	
28	940 P.2d 371 (Colo. 1997).....	19
	<i>Robinson Helicopter Co. v. Dana Corp.</i> ,	
	34 Cal. 4th 979 (2004)	12, 13
	<i>Rudolph v. Hudson's Bay Co.</i> ,	
	2019 WL 2023713 (S.D.N.Y. May 7, 2019)	16
	<i>Schnabel v. Trilegiant Corp.</i> ,	
	697 F.3d 110 (2d Cir. 2012)	16
	<i>Socal Recovery, LLC v. City of Costa Mesa</i> ,	
	2019 WL 1090774 (C.D. Cal. Jan. 29, 2019)	28

TABLE OF AUTHORITIES (cont'd.)**Page(s)**

1	<i>Spinks v. Equity Residential Briarwood Apartments</i> ,	
2	171 Cal. App. 4th 1004 (Cal. Ct. App. 2009)	18
3	<i>Stallone v. Farmers Group, Inc.</i> ,	
4	2022 WL 10091489 (D. Nev. Oct. 15, 2022)	4, 5, 8, 9
5	<i>Stasi v. Inmediata Health Grp. Corp.</i> ,	
6	501 F. Supp. 3d 898 (S.D. Cal. 2020).....	12, 13, 17, 25
7	<i>Sutter Health v. Superior Court</i> ,	
8	227 Cal. App. 4th 1546 (Cal. Ct. App. 2014)	20, 26
9	<i>TransUnion LLC v. Ramirez</i> ,	
10	141 S. Ct. 2190 (2021).....	5, 6
11	<i>US Fax L. Ctr., Inc. v. iHire, Inc.</i> ,	
12	374 F. Supp. 2d 924 (D. Colo. 2005), <i>aff'd</i> , 476 F.3d 1112 (10th Cir. 2007).....	23
13	<i>Vernon v. Qwest Commc 'ns Int'l. Inc.</i> ,	
14	857 F. Supp. 2d 1135 (D. Colo. 2012).....	17
15	<i>Wallace v. Health Quest Sys., Inc.</i> ,	
16	2021 WL 1109727 (S.D.N.Y. March 23, 2021)	21
17	<i>Walters v. Kimpton Hotel & Restaurant Group, LLC</i> ,	
18	2017 WL 1398660 (N.D. Cal. Apr. 13, 2017).....	7, 15

STATUTES

19	28 U.S.C.	
20	§ 2201	28
21	Cal. Civ. Code	
22	§ 56.06(b).....	26
23	§ 1798.140(c).....	24
24	Colo. Rev. Stat.	
25	§ 6-1-716(2)	27
26	§ 6-1-716(4)	27
27	New York General Business Law	
28	§ 349	14, 23
	§ 349(h).....	14
	New York Public Law 111-5	
	Section 13402(H)(2)	11

RULES

	Federal Rules of Civil Procedure	
	Rule 57	27

INTRODUCTION

Illuminate’s Motion to Dismiss (“MTD”)¹ should be denied because it rests on faulty arguments that have been repeatedly rejected by federal trial and appellate courts in the data breach context. Not only have Plaintiffs adequately demonstrated their standing through a host of viable legal theories recognized by courts in this Circuit, but Illuminate fails to address the gravity of its conduct as it specifically pertains to children. A child’s school records, or diagnosis of a learning disability, is of the utmost personal and sensitive information—even more so than an adult’s credit card numbers that can be quickly changed. And Illuminate’s cagey, dilatory, and evasive disclosures about the breach have only compounded the distress of Plaintiffs and other families and caused them further harm. Plaintiffs have adequately pleaded viable statutory and common law causes of action that warrant denial of Illuminate’s MTD.

FACTUAL BACKGROUND

Illuminate is a for-profit software company focused on youth education that earns revenue through contracts with public schools and school districts paid for by taxpayers. It services approximately 17 million students in 5,200 schools and districts across all 50 states. Illuminate has several product platforms in use at American schools that require the collection of all types of student data (much of which is highly sensitive and not public) including, among other things, students’ attendance and grades, birth dates, behavioral records, health records (such as student immunization, vision and hearing screening results); whether they qualify for special education; and socio-economic information such as whether they qualify for free or reduced-priced lunches. ¶¶ 5, 11, 32.² It also collects and stores various types of demographic information, as well as mail and email addresses, system usernames

¹ MTD refers to Illuminate’s Motion to Dismiss, Dkt. #61, filed on January 6, 2023.

² ¶ _ refers to a paragraph in the Consolidated Class Action Complaint. Dkt. # 57.

1 and passwords. ¶¶ 5, 32, 52. Illuminate is entrusted to protect the data it collects and
2 stores.³

3 Illuminate assured schools and parents that: (i) it was “deploy[ing] meaningful
4 safeguards to protect student data” that were in alignment with the Family
5 Educational Rights and Privacy Act (“FERPA”); (ii) its “systems are protected by
6 technological measures to help prevent unauthorized individuals from gaining
7 access” to student’s information; and (iii) it took measures to secure student data in
8 accordance with “contract[s] between Illuminate and your Educational
9 Organization.” Indeed, Illuminate went so far as to state that the measures it took to
10 safeguard and protect student data “meet or exceed the requirements of federal and
11 state law” and that its “employees are trained to observe and comply with applicable
12 federal and state privacy laws in the handling, processing, and storage of your
13 information.” ¶ 45.

14 Furthermore, in February 2016, Illuminate signed the Student Privacy Pledge
15 (the “Pledge”) created by the “Future of Privacy Forum,” (“FPF”) where it
16 represented to schools, students and parents that it would: (1) provide “a secure online
17 environment with data privacy securely in place”; and (2) promote “that student data
18 be safeguarded...” and further stated that its signing of the Student Privacy Pledge
19 “will give parents and educators confidence that data privacy safeguards are in place
20 when using Illuminate!” ¶¶ 46-50.

21 Despite its repeated promises that it was protecting the highly sensitive data
22 with which it was entrusted, Illuminate’s failures created a data breach calamity.
23 While Illuminate claims that it learned on January 8, 2022 of “suspicious activity” in
24 certain of its databases containing potentially protected student information (the
25 “Breach”), it was not until late March 2022 that it first notified schools that certain
26 of its databases containing potentially protected student information “were subject to
27

28 ³ Collectively, this data is referred to as “PI/PHI”

1 unauthorized access between December 28, 2021 and January 8, 2022.” And,
 2 notwithstanding its claim that its investigation purportedly confirmed the breach by
 3 March 24, 2022, Illuminate did not send legally-required data breach notification
 4 letters to some members of the Class, including Plaintiffs herein, until as late as
 5 July 29, 2022, more than four months after its purported confirmation of the Breach.
 6 ¶¶ 6, 8, 10, 19, 20.⁴ Illuminate’s delays in notifying certain school districts and
 7 parents of the Breach increased the risk of harm by depriving class members of the
 8 ability to promptly take steps to mitigate against potential adverse consequences of
 9 the Breach. ¶¶ 163,164.

10 Unknown at the time was just how egregious the nature and scope of the
 11 Breach was. The Breach has potentially affected more than 3 million former and
 12 current students nationwide, going back as far as 2016, and included some of the
 13 largest school districts in the country. Reports suggest that in New York alone, over
 14 1.9 million students have had their PI/PII disclosed. In California, over 500,000
 15 students from dozens of school districts have been affected. Tens of thousands of
 16 students from schools in Colorado, Oklahoma, Washington State and Connecticut
 17 have also been affected by the Breach, and there might be more to come. ¶¶ 30, 31.
 18 Indeed, one expert who tracks school cybersecurity incidents stated, with respect to
 19 New York school districts and the Breach: “I can’t think of another school district
 20 that has had a student data breach of that magnitude stemming from one incident.” ¶
 21 12. Subsequent to the Breach, Illuminate was also the first company to be removed
 22 from the Pledge. FPF noted that based on its review of the situation it appeared that
 23 Illuminate failed to meet its commitments and obligations to employ practices
 24
 25

26 ⁴ See also, Declaration of Devin S. Anderson in Support of Defendant Illuminate
 27 Education, Inc.’s Application to File Documents Under Seal Pursuant to Local
 28 Rule 79-5.2.2 In Support of its Motion to Dismiss the Consolidated Complaint
 (“Anderson Decl.”) at Exhibits 1, 2 and 3 (Data Breach Notification Letters from
 Illuminate dated July 29, 2022 and April 29, 2022). Dkt. # 63.

1 required of it to protect student data, including its apparent failure to encrypt student
2 data. ¶¶ 51-53.⁵

3 As discussed below, each of the Plaintiffs (who are parents of students and
4 their legal guardians) received notification from Illuminate and/or the school their
5 children attend or attended, that information concerning their children was
6 compromised by the Breach.

7 ARGUMENT

8 **I. PLAINTIFFS HAVE ADEQUATELY ALLEGED ARTICLE III** 9 **STANDING**

10 Illuminate argues that Plaintiffs have failed to plead facts to establish they have
11 Article III standing. Illuminate is wrong. It is well settled that “Standing under
12 Article III of the Constitution requires that an injury be concrete, particularized, and
13 actual or imminent; fairly traceable to the challenged action; and redressable by a
14 favorable ruling.” *Stallone v. Farmers Group, Inc.*, 2022 WL 10091489 at *3 (D.
15 Nev. Oct. 15, 2022) (quoting *Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139,
16 149 (2010)). And, “[a]t the pleading stage, ‘general factual allegations of injury
17 resulting from defendant’s conduct may suffice.’” *Stallone*, 2022 WL 10091489, at
18 *3, quoting *Mecinas v. Hobbs*, 30 F.4th 890, 897 (9th Cir. 2022). Plaintiffs’
19 allegations more than meet this standard.

20 **A. Plaintiffs Pleaded Concrete Injuries**

21 Plaintiffs sufficiently allege concrete injuries resulting from the Breach. As
22 demonstrated below, Plaintiffs injuries are more than hypothetical—they are real
23 injuries that are regularly held to confer standing by courts in the Ninth Circuit and
24 elsewhere.

25 **1. An Increased Risk of Harm from Identify Theft**

26 The Ninth Circuit, as well as some of its sister courts, have long held that in

27
28 ⁵ Additional allegations concerning Illuminates failure to comply with industry and
regulatory standards are listed at ¶¶ 55-64, 145-147, 150.

1 the context of data breach cases, allegations of an increased risk of future harm is
 2 sufficient to confer standing. *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1143 (9th
 3 Cir. 2010) (“Because the plaintiffs had alleged an act that increased their risk of
 4 future harm, they had alleged an injury-in-fact sufficient to confer standing.”); *In re*
 5 *Zappos.com, Inc. Customer Data Security Breach Litig.*, 888 F.3d 1020, 1027 (9th
 6 Cir. 2018) (Threat of future harm can confer standing, especially when considering
 7 the sensitivity of the type of information accessed in the breach.); *Stallone*, 2022 WL
 8 10091489, at * 4 (same). Indeed, as the Court in *Zappos* noted: “[p]resumably, the
 9 purpose of the hack is, sooner or later, to make fraudulent charges or assume those
 10 consumers’ identities.” *Zappos*, 888 F.3d at 1026 n.6 (quoting *Remijas v. Neiman*
 11 *Marcus Grp., LLC*, 794 F.3d 688, 693 (7th Cir. 2015)). Even Illuminate concedes
 12 that “courts in the Ninth Circuit [have] held that an ‘impending risk of identity theft’
 13 was sufficient for Article III Standing...” MTD at 9. Illuminate nevertheless argues
 14 that standing based on allegations of risk of future harm is not viable after the
 15 Supreme Court’s decision in *TransUnion LLC v. Ramirez*, 141 S. Ct. 2190 (2021).
 16 *Id.* Recent decisions in data breach cases—post-*TransUnion*—confirm that
 17 Illuminate is wrong. Illuminate suggests Plaintiffs could not have sustained injury
 18 because there is no allegation that financial, or credit card information of the children
 19 was provided to Illuminate. *See* MTD at 6 and 11. That is not the standard. Rather, it
 20 is the “sensitivity of the personal information” exposed by the breach that is
 21 determinative. *Stallone*, 2022 WL 10091489, at * 4-5.

22 Indeed, the Third Circuit, following *TransUnion*’s guidance recently held that
 23 “misuse [of the data at issue] is not necessarily required” and that increased risk of
 24 identity theft can confer standing. *Clemens v. ExecuPharm Inc.*, 48 F. 4th 146, 154-
 25 156 (3d Cir. 2022). The Court in *Clemens* also stated that “[w]e are content for now
 26 that the exposure of the type of information that was alleged here—information
 27 employees would normally choose to keep to themselves and would reasonably not
 28 want to make publicly available—and the resulting substantial risk of identity theft or

1 fraud is a harm that bears at least a ‘close relationship’ to harms traditionally
 2 recognized in privacy torts.” *Id.* (citations omitted). Plaintiffs submit that the type of
 3 sensitive information at issue here is at least as sensitive as the information at issue
 4 in *Clemens*. “Accordingly, the asserted injury supports Article III standing...” *Id.*

5 In *In re Blackbaud*, a case very similar to this one, (including that plaintiffs’
 6 alleged injuries were similar to those at issue here), Defendant moved to dismiss,
 7 arguing that plaintiffs lacked Article III standing. *In re Blackbaud, Inc. Customer*
 8 *Data Breach Litig.*, 2021 WL 2718439, at *3 (D.S.C. July 1, 2021). In denying the
 9 motion and finding that plaintiffs had adequately alleged standing, the *Blackbaud*
 10 Court stated that the *TransUnion* decision “would not impact the court’s injury in
 11 fact analysis at this stage of the litigation” and in doing so further noted that the
 12 *TransUnion* decision was based on a much more developed record in that case and,
 13 therefore, not particularly relevant to a motion to dismiss. *Id.* at *3, 5-6, 8, and fn. 15.

14 Here, every Plaintiff has alleged an increased risk of identity theft due to
 15 Illuminate’s failure to protect the data it was entrusted with. *See* ¶¶ 35-37, 42, 72,
 16 82, 94, 106, 118, 130, 158. Each Plaintiff has alleged that this situation has caused
 17 them emotional distress. ¶¶ 71, 81, 93, 105, 117, 129. *See McKenzie v. Allconnect,*
 18 *Inc.*, 369 F. Supp. 3d 810, 816 (E.D. Ky. 2019) (finding that plaintiffs allegations
 19 that they suffered emotional distress as a result of the unauthorized release of
 20 personal data, as well as having to expend time to mitigate the risk of identity theft
 21 resulting from the breach, were sufficient to confer standing.).

22 Concerns about the hacked data resulting in identity theft are heightened in
 23 this case given that children’s data is particularly attractive to data thieves and can
 24 have long-lasting effects on a child’s financial history and identity. *See* ¶¶ 35-37,
 25 39-43. Indeed, as one cybersecurity professional stated in reference to the Illuminate
 26 breach: “If you’re a bad student and had disciplinary problems and that information
 27 is now out there, how do you recover from that?... It’s your future. It’s getting into
 28 college, getting a job. It’s everything.” ¶ 43. Further highlighting the real risk to

1 Plaintiffs from the Breach, the New York Times reported that the vice president for
 2 a cybersecurity risk management firm, during an interview on the Illuminate Data
 3 Breach, was able to find one of Illuminate’s Amazon Web Services (“A.W.S.”)
 4 buckets [a service Illuminate used] with an easily guessable name and the reporter
 5 interviewing him was able to find a second A.W.S. bucket. ¶ 34

6 As Illuminate acknowledges, there are allegations that at least two of the
 7 Plaintiffs have experienced some form of “hacking” since the Breach, but argue
 8 these allegations are insufficient for standing purposes. MTD at 7-8. *See* ¶¶ 103,
 9 115. Illuminate also argues that “Plaintiffs have not plausibly alleged any actual
 10 identity theft as a result of their information being potentially subject to access in
 11 the cyberattack.” MTD at 7. Defendants in other data breach cases have similarly
 12 argued that there can be no standing without allegations of actual identity theft.
 13 Courts within the Ninth Circuit have rejected that argument. *Walters v. Kimpton*
 14 *Hotel & Restaurant Group, LLC*, 2017 WL 1398660, at *1 (N.D. Cal. Apr. 13, 2017)
 15 (citing to cases within the Ninth Circuit and holding “[t]he Court respectfully
 16 disagrees that a plaintiff must actually suffer the misuse of his data or an
 17 unauthorized charge before he has an injury for standing purposes.”).

18 Finally, in support of its arguments, Illuminate repeatedly cites to *I.C. v.*
 19 *Zynga, Inc.*, 2022 WL 2252636, *7-8 (N.D. Cal. Apr. 29, 2022) (“*Zynga*”). The facts
 20 alleged in *Zynga*, however, are clearly distinguishable from those alleged in this case.
 21 Unlike here, where the information compromised concerning students was of an
 22 incredibly sensitive and confidential nature (*i.e.*, learning disabilities, medical
 23 information, socio-economic and behavioral records and grades), in *Zynga*
 24 compromised data was essentially basic contact information, usernames, passwords
 25 to gaming accounts—all of which, as the *Zynga* Court noted, is the type of
 26 information that can be changed by users. Indeed, the *Zynga* Court stated that
 27 “Plaintiffs have not demonstrated that the information stolen was of a nature that
 28

1 disclosure or intrusion thereupon would be highly offensive to the reasonable
2 person.” *Id.* at *7-8.

3 **a. Illuminate’s Notification Letter to Plaintiffs Concede**
4 **Their Risk of Future Harm**

5 As noted above, after the Breach Illuminate sent data breach notification letters
6 to certain Plaintiffs. In such letters Illuminate encourages Plaintiffs to take various
7 steps to protect themselves in light of the Breach, including enrolling in credit and
8 identity monitoring services, be “vigilant against incidents of identity theft and fraud
9 by reviewing your account statements” and even recommended, among other things,
10 review of your minor’s account statements from the past 12 to 24 months.⁶ ¶¶ 153-
11 54. *See also* Anderson Decl. at Exhibits 1, 2 and 3 (Illuminate’s Data Breach
12 notification letters to Plaintiffs).

13 **2. Plaintiffs’ Allegations of Diminished Value of Their PI/PHI**
14 **is a Concrete Injury**

15 Plaintiffs allege that they suffered actual injury in the form of damages due to
16 diminution of the value of their PI/PHI as a result of the Breach. ¶¶ 69, 79, 91, 102,
17 114, 127. Indeed, “Diminution in value of personal information can be a viable theory
18 of damages.” *Stallone*, 2022 WL 10091489, at *6, quoting *Pruchnicki v. Envision*
19 *Healthcare Corp.*, 439 F.Supp.3d 1226, 1234 (D. Nev. 2020), *affirmed* 845 Fed.
20 App’x 613 (9th Cir. 2021); *In re Yahoo! Inc. Customer Data Security Breach Litig.*,
21 2017 WL 3727318, at *13-14 (N.D. Cal. Aug. 30, 2017) (loss in value of PI is an
22 injury in fact for standing purposes). Illuminate nevertheless argues that Plaintiffs’
23 allegations of injury based on diminished value of their private information are
24 insufficient to confer standing. MTD at 12. Such arguments have been repeatedly
25 rejected by Courts in this and other Circuits. *Stallone*, 2022 WL 10091489, at *6

26 _____
27 ⁶ Notably, Illuminate submitted its data breach notification letters to certain Plaintiffs
28 under seal, admitting that “Public release of this information could compromise the
security of the students’ identities and their privacy...” Dkt. # 62. The Court granted
the motion. Dkt. # 64.

1 (“[T]hat a plaintiff must establish both the existence of a market for their PII and an
 2 impairment of their ability to participate in that market is not supported by Ninth
 3 Circuit precedent[.]”.

4 **3. Plaintiffs’ Loss of Time and/or Money Expended to Mitigate** 5 **the Risk of Harm Confers Standing**

6 Illuminate also argues that the allegations of time and/or expense spent by
 7 Plaintiffs to mitigate the potential harmful impact to themselves and their children
 8 are insufficient to confer standing. MTD at 11-12. Defendant is wrong. Courts in
 9 this Circuit and elsewhere have recognized that loss of time and/or expense spent to
 10 mitigate the impact of a data breach can constitute a concrete injury for standing
 11 purposes. *In re Anthem, Inc. Data Breach Litig.*, 2016 WL 3029783, at *25-26 (N.D.
 12 Cal. May 27, 2016).

13 Plaintiffs here have alleged how they have suffered loss of time (including the
 14 number of hours expended), and inconvenience dealing with the consequences of the
 15 Breach and/or taking steps to mitigate potential harm from it. ¶¶ 68, 90, 113,
 16 126, 157.

17 **4. Plaintiffs Have Been Further Injured by Illuminate’s Delay**

18 Courts in this Circuit have also held that allegations of incremental harm
 19 caused by a defendant’s delay in notifying plaintiffs of a data breach can constitute
 20 an injury for standing purposes. *Stallone*, 2022 WL 10091489, at *8. (“[C]ourts
 21 within the Ninth Circuit have found that plaintiffs adequately pled incremental harm
 22 when plaintiffs plausibly alleged that they could not take mitigation steps due to
 23 defendants delay in notifying them of a data breach.”). Plaintiffs here have alleged
 24 that Defendant’s delay in identifying and notifying them of the Breach has caused
 25 them additional harm. ¶¶ 161-165.

26 **II. CHOICE OF LAW**

27 Illuminate argues that rather than applying California law to a nationwide
 28 class, the Court should apply the law of the individual plaintiffs’ states of residence.

MTD at 13. The Court need not address the choice of law issue at this stage of the litigation. *Clancy v. The Bromley Tea Co.*, 308 F.R.D. 564, 572-73 (N.D. Cal. 2013) (“Such a detailed choice-of-law analysis is not appropriate at this stage of the litigation. Rather, such a fact-heavy inquiry should occur during the class certification stage, after discovery.”); *see also In re Clorox Consumer Litig.*, 894 F. Supp. 2d 1224, 1237 (N.D. Cal. 2012) (“Since the parties have yet to develop a factual record, it is unclear whether applying different state consumer protection statutes could have a material impact on the viability of Plaintiffs’ claims.”); *Morrison v. Ross Stores*, 2019 WL 11770849, at *1 (N.D. Cal. May 30, 2019) (“The choice-of-law question is one that must be answered in the context of class certification.”).

However, if the Court is inclined to decide the choice-of law issue at this stage, it should apply California law to the proposed nationwide Class because much of the conduct at issue in this case emanated from California. ¶¶ 167-169 (headquarters, “nerve center”, decisions, and breach all in California). Accordingly, California law should also apply to out-of-state plaintiffs in this case. *Morrison*, 2019 WL 11770849, at *1; *see also Ehret v. Uber Techs., Inc.*, 68 F.Supp.3d 1121, 1131-32 (N.D. Cal. 2014) (California statutes apply extraterritorially when conduct emanated from California); *In re iPhone 4S Consumer Litig.*, 2013 WL 3829653, at *7-9 (N.D. Cal. July 23, 2013) (same); *In re Clorox Consumer Litig.*, 894 F.Supp.2d at 1237-38 (same).

III. PLAINTIFFS HAVE ADEQUATELY PLEADED CAUSES OF ACTION FOR NEGLIGENCE

A. Illuminate Was Negligent, As Evidenced By The Data Breach

Specific failures on the part of Defendant amounting to a plausible claim for negligence are adequately alleged in the Complaint. ¶¶ 53, 55, 64 (failure to implement the security measures; protection against any possible communication system; and training staff regarding critical points); ¶ 147 (failure to remove old,

1 unused or obsolete data of former students; failure to encrypt such information);
 2 ¶ 163 (delaying four to seven months in providing notice of the data breach); ¶ 190
 3 (providing untimely and insufficient notice of the data breach); ¶ 191(c) (failure to
 4 securely delete the children's unneeded data, pursuant to COPPA); ¶ 191(d)
 5 (disclosing PII to unauthorized third-parties; failure to employ encryption
 6 technology using a technology or methodology specified by the secretary of the
 7 United States Department of Health and Human services in guidance issued under
 8 Section 13402(H)(2) of New York Public Law 111-5, in violation of the New York
 9 State Education Law); ¶ 193(e) (failure to provide timely notice of a data breach);
 10 and ¶ 193(f) (failure to provide adequate notice of the data breach).

11 Defendant's authorities to the contrary are distinguishable. MTD at 15. In *In*
 12 *re Waste Mgmt. Data Breach Litig.*, 2022 WL 561734, at *4 (S.D.N.Y. Feb. 24, 2022)
 13 the court dismissed the plaintiffs' negligence claim because unlike Plaintiffs'
 14 complaint as stated above, the complaint failed to plead any facts "regarding any
 15 specific measures that Waste Management did or didn't take" or how "their systems
 16 were breached." In *Cnty. Bank of Trenton v. Schnuck Markets, Inc.*, 887 F.3d 803,
 17 818 (7th Cir. 2018) the court dismissed the negligence claim because it applied the
 18 economic loss doctrine since the plaintiff banks were involved in a network of
 19 contracts with the defendant, and, unlike Plaintiffs here, the plaintiff banks were not
 20 consumers but financial institutions. Plaintiffs argue in Section B below that the
 21 economic loss doctrine does not preclude Plaintiffs' negligence claims. Moreover,
 22 Defendant's authorities are distinguishable because here, as stated above,
 23 "[P]laintiffs...plausibly allege not only that there was a data breach, but that the
 24 breach was caused by [Illuminate]'s unreasonable conduct."⁷ *In re Waste Mgmt.*,

25
 26
 27 ⁷ *Cnty. Bank of Trenton* is also distinguishable because there, the court held that
 28 Illinois and Missouri do not recognize a duty in the context of data breaches. *Cnty.*
Bank of Trenton, 887 F.3d at 818.

2022 WL 561734, at *5. For these same reasons, it is incorrect to state that Plaintiffs are relying solely upon the doctrine of *res ipsa loquitur*. MTD at 15.

B. The Economic Loss Doctrine Does Not Preclude Plaintiffs' Negligence Claims

“[T]he economic loss rule prevents the law of contract and the law of tort from dissolving one into the other” and “requires a [plaintiff] to recover in contract for purely economic loss due to disappointed expectations, unless he can demonstrate harm above and beyond a broken contractual promise.” *Robinson Helicopter Co. v. Dana Corp.*, 34 Cal. 4th 979, 988 (2004) (brackets and internal quotation marks omitted). In other words, “[u]nder the economic loss doctrine, a plaintiff’s tort recovery of economic damages is barred unless such damages are accompanied by some form of physical harm (*i.e.*, personal injury or property damage).” *In re Sony Gaming Networks & Customer Data Sec. Breach Litig.*, 903 F. Supp. 2d 942, 961 (S.D. Cal. 2012) “Thus, in actions for negligence, liability is limited to damages for physical injuries and recovery of economic loss is not allowed.” *Id.* (citations omitted). Therefore, to recover a purely economic loss a plaintiff must allege “(1) personal injury, (2) physical damage to property, (3) a special relationship existing between the parties, or (4) some other common law exception to the rule.” *Kalitta Air, L.L.C. v. Cent. Texas Airborne Sys., Inc.*, 315 F. App’x 603, 605 (9th Cir. 2008) (internal quotation marks omitted).

Here, Plaintiffs have plausibly pleaded non-economic damages. *See* ¶ 148 (loss of privacy and information, loss of time and money related to identity theft); ¶¶ 71, 81, 93, 105, 117, 129, 242 (emotional distress); ¶¶ 72, 82, 103, 115, 131 (increased spam). Thus, “Plaintiffs have alleged they have lost time responding to the Breach as well as suffering from increased anxiety and so do not allege purely economic losses.” *In re Solara Med. Supplies, LLC Customer Data Sec. Breach Litig.*, 2020 WL 2214152, at *4 (S.D. Cal. May 7, 2020); *Stasi v. Inmediata Health Grp. Corp.*, 501 F. Supp. 3d 898, 913 (S.D. Cal. 2020) (“Plaintiffs allege they noticed an increase

1 in spam/phishing e-mails and/or calls...which is harm that is also not necessarily
2 ‘economic’ in nature.”).

3 Even if the Court were to find that Plaintiffs only alleged economic loss, the
4 economic loss doctrine would not apply here because a “special relationship” exists
5 between Plaintiffs and Illuminate, an exception that removes Plaintiffs’ claims from
6 the purview of the economic loss doctrine.⁸ To assess the existence of a special
7 relationship giving rise to an independent duty, courts have considered six factors:
8 (1) the extent to which the transaction was intended to affect the plaintiffs; (2) the
9 foreseeability of harm to the plaintiffs; (3) the degree of certainty that the plaintiffs
10 suffered injury; (4) the closeness of the connection between the defendant’s conduct
11 and the injury suffered; (5) the moral blame attached to the defendant’s conduct; and
12 (6) the policy of preventing future harm. *Huynh v. Quora, Inc.*, 508 F. Supp. 3d 633,
13 654-55 (N.D. Cal. 2020) (citing *J’Aire Corp. v. Gregory*, 24 Cal. 3d 799, 804 (1979)).
14 “All six factors must be considered by the court and the presence or absence of one
15 factor is not decisive.” *Id.* (citations omitted). To the extent necessary for Plaintiffs
16 to recover economic losses, Plaintiffs easily satisfy the *J’Aire* factors.

17 C. Negligence *Per Se* Has Been Plausibility Pleaded

18 Plaintiffs adequately allege they are entitled to an evidentiary presumption of
19 negligence *per se* based on violations of various statutes. “Under California law,
20 [Illuminate’s] failure to exercise due care is presumed if Plaintiffs sufficiently allege
21 that: (1) [Illuminate] violated a statute or regulation; (2) the violation was the
22 proximate cause of Plaintiffs’ injury; (3) the injury resulted from an occurrence, the
23 nature of which the statute or regulation was designed to prevent; and (4) the person
24 suffering the injury was one of the class of persons for whose protection the statute
25 or regulation was adopted. *Stasi*, 501 F. Supp. 3d at 919 (citing Cal. Evid. Code

26
27 ⁸ Further, to the extent that Defendant has argued that there is no contractual
28 relationship between Illuminate and Plaintiffs, and should the Court agree with
Defendant, the economic loss doctrine need not even be considered. *See Robinson
Helicopter Co.*, 34 Cal. 4th at 988.

§ 669). Furthermore, “Plaintiffs’ reliance on the negligence *per se* doctrine does not fail merely because the statutes they allege Defendants violated do not provide a private right of action[,]” as “Plaintiffs are not attempting to sue under these statutes.” *In re Ambry Genetics Data Breach Litig.*, 567 F. Supp. 3d 1130, 1142-43 (C.D. Cal. 2021). “Rather, the statutes instead serve the subsidiary function of providing evidence of an element of a pre-existing common law cause of action.” *Id.* at 1142 (internal citations and quotations omitted).

Similarly, under New York law, violation of a statute may constitute negligence *per se* if the injured party belongs to the class of persons that the statute was intended to protect, and the injury is of the type from which the statute was intended to protect. *Feldman v. CSX Transp., Inc.*, 31 A.D.3d 698, 821 N.Y.S.2d 85 (2d Dep’t 2006). Here, the FTC Act (§ 207), FERPA (§ 208), HIPAA (§ 209), CCPA (§ 210), and COPPA (§ 211) are all statutes intended to protect persons similarly situated to Plaintiffs from the same sort of injury alleged herein. Defendant’s citation of *Lugo v St. Nicholas Assoc.*, 772 N.Y.S.2d 449, 453 (N.Y. Sup. Ct. 2003) in support of the proposition that “a negligence *per se* claim cannot be based on a statute that itself lacks a private right of action” is selective at best. MTD at 17. In *Lugo*, the court held that “although a statute does not provide for a private right of action, its standard of care may be relevant for purposes of a negligence action[.]” *Lugo*, 772 N.Y.S.2d at 453. Furthermore, Defendant fails to acknowledge that Count XIII of the Complaint alleges violation of New York General Business Law §349 which provide for a private right of action for damages. § 349(h) (“any person who has been injured by reason of any violation of this section may bring an action in his own name”). Likewise, as discussed below, the Colorado statutes provide a private right of action. *See* Section VII.C.

IV. PLAINTIFFS STATE A CLAIM FOR BREACH OF CONTRACT

Illuminate’s argument that Plaintiffs’ claim for breach of contract fails because Plaintiffs failed to “establish that a contract existed between plaintiffs and Illuminate,

1 the terms of the contract, and fail to show that Illuminate’s contract with the school
 2 districts was intended to benefit plaintiffs, is completely without merit. MTD at 18-
 3 20. Clearly, Illuminate intended to benefit Plaintiffs and the Class when it came into
 4 possession of the PI/PHI through contracts that it entered into with the students’
 5 school districts, pursuant to which it stored the students’ PI/PHI. MTD at 18-20;
 6 ¶¶ 14, 246. Here, Illuminate agreed to maintain Plaintiffs’ privacy in accordance with
 7 FERPA and otherwise, in its Privacy Policy, Pledge, and related policies and
 8 statements. ¶¶ 44-50; 245. Illuminate also states on its website that “[i]n alignment
 9 with [FERPA], we deploy meaningful safeguards to protect student data” and [W]e
 10 pledge our unwavering commitment to student data privacy.” ¶48. Additionally,
 11 Illuminate assured Plaintiffs of its legal duties and privacy practices with respect to
 12 Plaintiffs’ Private Information in its Notice of Privacy Practices on its website,
 13 contracts with school districts and signing the Pledge in February 2016. ¶¶ 44-50.
 14 Illuminate’s intent to benefit Plaintiffs and the Class is further bolstered by the fact
 15 that it provided data breach notices directly to some Plaintiffs and class members that
 16 stated “[t]he confidentiality, privacy, and security of information in our care is among
 17 our highest priorities.” Anderson Decl. at Exhibits 1, 2 and 3.

18 The above allegations are sufficient to show an implied contract.⁹ *See, e.g.,*
 19 *Walters*, 2017 WL 1398660, at *2 (implied contract arose from privacy policy when
 20 it was “committed” to safeguarding customer privacy and personal information).
 21 Contrary to its assertions, Illuminate then breached that contract by failing to provide
 22 adequate security for Plaintiffs’ PI/PHI. ¶¶ 13, 29, 34, 53, 147; *In re Premera Blue*
 23 *Cross Customer Data Security Breach Litig.*, 2017 WL 539578, *6, 11 (D. Ore.
 24 Feb. 9, 2017) (denying motion to dismiss contract claims based on privacy notice in
 25

26 ⁹ Plaintiffs concede that they were not parties to an express written contract with
 27 Illuminate. Rather, they were foreseeable third-party beneficiaries of the contracts
 28 between Illuminate and the various school districts, and Illuminate’s representations
 created implied contracts. *See Stasi*, 501 F.Supp.3d at 920; *see also* ¶¶ 13, 29, 34, 53,
 44-50, 147, 245.

1 data breach case). Illuminate’s argument that “plaintiffs fail to identify any contract
 2 with Illuminate” and that “[i]t is not enough to merely point to a privacy policy,
 3 without other allegations that plausibly show mutual assent” fails for the same reason.
 4 MTD at 18; ¶¶ 44-50 (allegations detailing Illuminate’s assurances to Plaintiffs); *In*
 5 *re Yahoo! Inc. Customer Data Sec. Breach Litig.*, 2017 WL 3727318, at *44, 47
 6 (N.D. Cal. Aug. 30, 2017); *Hameed-Bolden v. Forever 21 Retail, Inc.*, 2018 WL
 7 6802818, at *3 (C.D. Cal. Oct. 1, 2018) (finding implied contract where defendant
 8 failed to safeguard information); *Gordon v. Chipotle Mexican Grill, Inc.*, 344 F.
 9 Supp. 3d 1231, 1247–48 (D. Colo. 2018) (same); *Rudolph v. Hudson’s Bay Co.*, 2019
 10 WL 2023713, at *11 (S.D.N.Y. May 7, 2019) (same).

11 Cases Illuminate cites do not hold otherwise. While the court in *Cohen v. Ne.*
 12 *Radiology, P.C.*, 2021 WL 293123, at *9 (S.D.N.Y. Jan. 28, 2021) did not find that
 13 there was an express contract between plaintiff and defendants, the court found an
 14 implied contract existed based on plaintiff’s allegations that defendants “obtained,
 15 created, and maintained e-PHI as part of providing radiological services to their
 16 patients, evincing an implicit promise by defendants to protect their patients’ e-PHI
 17 from unauthorized users.” In fact, the court in *Cohen* found that defendants’ Notice
 18 of Privacy further supported an “implicit promise” to “safeguard” plaintiffs’ private
 19 information. *Id.* (citations omitted).

20 That the complaint does not contain allegations that Plaintiffs had “knowledge
 21 of or interaction with Illuminate” prior to the Breach and therefore there was no
 22 “mutual assent” (MTD at 19), is not fatal to Plaintiffs’ breach of contract claim since
 23 the complaint pleads that Illuminate promised on its website and in its Pledge that it
 24 would protect Plaintiffs’ private information, and it was this promise that formed the
 25 implied contract. Defendant’s cases are distinguishable since, unlike here, they are
 26 based on the construction of an arbitration clause to an existing contract. *Schnabel v.*
 27 *Trilegiant Corp.*, 697 F.3d 110, 120 (2d Cir. 2012) (on a motion to compel
 28 arbitration); *Berkson v. Gogo LLC*, 87 F. Supp. 3d 359, 392 (E.D.N.Y. 2015)

(application of an arbitration clause to an existing contract); *Vernon v. Qwest Commc'ns Int'l. Inc.*, 857 F. Supp. 2d 1135, 1150 (D. Colo. 2012) (consumers entering into contracts for services but not aware of the arbitration clause).

Finally, Defendant argues that Plaintiffs fail to plead the terms of the contract and fail to “attach or quote any contract.” MTD at 19. However, “[a] contract may be explained by reference to the circumstances under which it was made, and the matter to which it relates.” *Cummings v. Entergy Int'l Servs., LC*, 271 F. Supp. 3d 1182, 1189 (E.D. Cal. 2017). The court in *Stasi* upheld third party beneficiary contract claims of plaintiffs who are patients of health care providers who the defendant provides billing and health record software and service solutions to and stated “[a]lthough Plaintiffs do not provide specific contract terms, Plaintiffs allege the substance of the relevant terms...[and], without discovery, it is not clear what more Plaintiffs could plead[.]” *Stasi*, 501 F. Supp. 3d at 920.

Furthermore, “[t]he existence of an implied contract is an issue of fact” inappropriate for determination on a motion to dismiss. *Castillo v. Seagate Tech., LLC*, 2016 WL 9280242, at *8 (N.D. Cal. Sept. 14, 2016). Plaintiffs allege they entrusted Defendant with their Private Information, and that Defendant failed to safeguard it. ¶¶ 5, 11, 13, 29, 34, 53, 147. “When a person hands over sensitive information. . . , they presumably expect to receive an implicit assurance that the information will be protected.” *Castillo*, 2016 WL 9280242, at *9. Courts have found such allegations sufficient. Therefore, Plaintiffs have properly alleged a breach of implied contract and Defendant’s motion to dismiss the contract claim should be denied.

V. PLAINTIFFS STATE A CLAIM FOR INVASION OF PRIVACY

Plaintiffs assert invasion of privacy under both the California Constitution and common law. ¶¶ 220-229, 249-262. As the Ninth Circuit stated while reversing a dismissal of such claims, in order to state a claim Plaintiffs must allege “(1) there exists a reasonable expectation of privacy, and (2) the intrusion was highly

1 offensive.” *In re Facebook Internet Tracking Litig.*, 956 F.3d 589, 601 (9th Cir.
 2 2020) (citing *Hernandez v. Hillsides, Inc.*, 47 Cal. 4th 272, 286 (2009)). Both of these
 3 issues present “mixed questions of law and fact.” *Hill v. Nat’l Collegiate Athletic*
 4 *Assn.*, 7 Cal. 4th 1, 40 (1994).; *see also Facebook Internet Tracking*, 956 F.3d at 601.

5 Without addressing these elements, Defendant argues that Plaintiffs must
 6 allege an “intentional, egregious privacy invasion.” MTD at 21. Defendant cites *In*
 7 *re iPhone Application Litig.*, 844 F. Supp. 2d 1040, 1063 (N.D. Cal. 2012) (“*In re*
 8 *iPhone*”), for the proposition that Plaintiffs must plead intentional misconduct, but
 9 this case predates the Ninth Circuit’s opinion in *In re Facebook Internet Tracking*,
 10 where the Ninth Circuit specifically refused to follow *In re iPhone*. *See In re*
 11 *Facebook Internet Tracking*, 956 F.3d at 606 & n.8. Defendant also cites *Dugas v.*
 12 *Starwood Hotels & Resorts Worldwide, Inc.*, 2016 WL 6523428, at *12 (S.D. Cal.
 13 Nov. 3, 2016), on this point, but that court simply followed *In re iPhone* and, again,
 14 did not analyze the claim under the test enunciated by the Ninth Circuit in the later-
 15 decided *In re Facebook Internet Tracking*.

16 Defendant attempts to create a new element where one does not exist. There
 17 is no “heightened intent” requirement for Plaintiffs’ invasion of privacy claim.
 18 California law “makes no distinction” between intentional and negligent invasion of
 19 privacy. *Spinks v. Equity Residential Briarwood Apartments*, 171 Cal. App. 4th
 20 1004, 1043 (Cal. Ct. App. 2009). “The motives of a person charged with invading
 21 the [privacy] right are not material with respect to the determination whether there is
 22 a right of action, and malice is not an essential element of a violation of the right.”
 23 *Fairfield v. American Photocopy etc. Co.*, 138 Cal. App. 2d 82, 87 (Cal. Ct. App.
 24 1955).

25 Although not required to do so, Plaintiffs *have* alleged an intentional invasion
 26 of privacy claim against Defendant. Plaintiffs allege Defendant knew their
 27 information security practices were inadequate, that these inadequate data security
 28 measures would likely result in a data breach like the Breach and that Defendant

1 knew that such a Breach would harm Plaintiffs through release of their highly
 2 sensitive, immutable PI/PHI. ¶¶ 146, 258, 259; *see In re Ambry*, 567 F. Supp. 3d at
 3 1143 (court upheld plaintiffs common law invasion of privacy claim where plaintiffs
 4 alleged that defendants “knew their information security practices were inadequate
 5 and had numerous security vulnerabilities,” “intentionally, willfully, recklessly, or
 6 negligently’ failed to take adequate and reasonable measures to ensure Ambry’s data
 7 systems were protected,” “knew their inadequate data security measures would likely
 8 result in a breach” and “knew that such a breach would harm Plaintiffs”). (citations
 9 omitted).

10 Defendant acknowledges that both Colorado and California¹⁰ recognize the
 11 common law claim for invasion of privacy and dispute only the public disclosure
 12 requirement with respect to Plaintiffs’ claim. *Robert C Ozer, P.C. v. Borquez*,
 13 940 P.2d 371, 377 (Colo. 1997) (*en banc*); *Hill*, 7 Cal. 4th at 27. Here, Plaintiffs’
 14 have alleged that their PI/PHI that is now in the hands of identity thieves and cyber
 15 criminals will be posted on the dark web for years as well as openly posted directly
 16 on various illegal websites making this information publicly available. ¶ 143.
 17 Therefore, Plaintiffs’ allegations state a claim for invasion of privacy and the motion
 18 to dismiss should be denied.

19 **VI. PLAINTIFFS ADEQUATELY ALLEGE THEIR BREACH OF** 20 **CONFIDENCE CLAIM**

21 The elements of a breach of confidence claim are: “(1) the plaintiff conveyed
 22 ‘confidential and novel information’ to the defendant; (2) the defendant had
 23 knowledge that the information was being disclosed in confidence; (3) there was an
 24 understanding between the defendant and the plaintiff that the confidence be
 25 maintained; and (4) there was a disclosure or use in violation of the understanding.”
 26 *Ent. Rsch. Grp., Inc. v. Genesis Creative Grp., Inc.*, 122 F.3d 1211, 1227 (9th Cir.

27 _____
 28 ¹⁰ Plaintiffs concede that New York does not recognize the common law claim for
 invasion of privacy.

1 1997) (citations omitted). Defendant argues that “the lack of a contractual
 2 relationship” (MTD at 22-23) between Illuminate and Plaintiffs and that Illuminate’s
 3 disclosure of Plaintiffs’ Private Information was not voluntary (MTD at 23) are fatal
 4 to their breach of confidence cause of action.

5 First, as set forth above in Section IV., *supra*, Plaintiffs have established that
 6 they had an implied contract with Illuminate wherein Illuminate promised to “protect
 7 the Private Information and other data of current and former students... in
 8 accordance with the applicable Federal, State and local statutes and regulations...”
 9 ¶ 44. Specifically, on Illuminate’s website, it states that “We pledge our unwavering
 10 commitment to student data privacy. ¶ 45. Illuminate also signed the Pledge. ¶¶ 46,
 11 47. Defendant’s cases are distinguishable.¹¹ *Ent. Rsch. Grp., Inc.*, was decided on a
 12 motion for summary judgement after a trial had taken place. In *Pauwels v. Deloitte*
 13 *LLP*, 2020 WL 818742 at *8 (S.D.N.Y. Feb. 19, 2020) the plaintiff, unlike Plaintiffs
 14 here, failed to allege facts establishing the “existence of a confidential relationship.”
 15 Moreover, neither of these cases has anything to do with data breaches or alleged
 16 breach of confidence claims.

17 Second, Defendant’s argument that Plaintiffs “have not alleged Illuminate
 18 affirmatively disclosed this information in violation of plaintiffs’ confidence” and
 19 did not “voluntarily offer up” Plaintiffs’ Private Information is baseless. MTD at 22.
 20 Illuminate’s argument is predicated on an invented voluntary disclosure requirement.
 21 MTD at 23. While courts have rejected the claim where information was stolen,
 22 rather than intentionally disclosed, here, where Plaintiffs allege Illuminate knew that
 23 it failed to maintain reasonable and appropriate data security for Plaintiffs’ PI/PHI
 24 and being aware that it was a target for cybercriminals, the Court should conclude
 25 that Illuminate’s recklessness is sufficiently egregious and tantamount to voluntary
 26 disclosure for purposes of Plaintiffs’ breach of confidence claim.

27
 28 ¹¹ *Sutter Health v. Superior Court*, 227 Cal. App. 4th 1546, 1555-1556 (Cal. Ct. App. 2014) is distinguishable since the case did not involve a breach of confidence claim.

1 Indeed, courts have upheld breach of confidence claims in the data breach
 2 context where information was not intentionally disclosed. *See In re Cap. One*
 3 *Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 409 (E.D. Va. 2020) (breach
 4 of confidence claim on behalf of California plaintiffs sustained in data breach class
 5 action where defendant did not voluntarily disclose the breached information);
 6 *Wallace v. Health Quest Sys., Inc.*, 2021 WL 1109727, at *13 (S.D.N.Y. March 23,
 7 2021) (breach of confidence claim sustained where plaintiffs' sensitive information
 8 was potentially compromised and disclosed to cybercriminals).

9 Thus, Plaintiffs' allegations state a claim for breach of confidence and the
 10 motion to dismiss should be denied.

11 **VII. PLAINTIFFS' STATUTORY CLAIMS ARE ADEQUATELY** 12 **PLEADED**

13 **A. Plaintiffs Are Not Required To Prove Reliance Under The** 14 **Statutory Claims Alleged**

15 Illuminate's attacks on Plaintiffs' statutory claims are without merit. First,
 16 Illuminate claims that "Plaintiffs have not identified any specific claims made by
 17 Illuminate about its security that are false[.]" MTD at 24. That is wrong. Plaintiffs'
 18 Complaint specifically alleges that Illuminate claimed it will "protect your data like
 19 it's our own "[i]n alignment with...FERPA" and that these "measures meet or exceed
 20 the requirements of applicable federal and state law." ¶ 45. Illuminate further states
 21 it "deploy[s] meaningful safeguards to protect student data." *Id.* These statements
 22 provide "specific, non-subjective guarantee[s] that [Illuminate] uses safeguards that
 23 could protect the information it collects." *Huynh v. Quora, Inc.*, 2020 WL 7408230,
 24 at *11 (N.D. Cal. June 1, 2020) (citing *In re Yahoo!*, 2017 WL 3727318, at *26
 25 (finding the allegation that Defendant's statement that it had "physical, electronic,
 26 and procedural safeguards that comply with federal regulations to protect personal
 27 information about you" is actionable). As described in Section I above, Plaintiffs
 28 describe how these statements caused their injuries.

1 Second, Illuminate’s argument that Plaintiffs failed to plead reliance on these
 2 statements is a red herring because reliance is not required on their primary legal
 3 theories. MTD at 24. Plaintiffs do not allege a violation of the California Unfair
 4 Competition Law (“UCL”) under the fraudulent prong, rather, they allege violation
 5 under the unlawful and unfair prongs, and reliance is not required. ¶¶ 273-279. “The
 6 ‘unlawful’ prong of the UCL prohibits ‘anything that can properly be called a
 7 business practice and that at the same time is forbidden by law.’” *In re Adobe Sys.,*
 8 *Inc. Priv. Litig.*, 66 F. Supp. 3d 1197, 1225 (N.D. Cal. 2014) (citations omitted). “By
 9 proscribing ‘any unlawful’ business practice, the UCL permits injured consumers to
 10 ‘borrow’ violations of other laws and treat them as unlawful competition that is
 11 independently actionable.” *Id.* As predicates for their claim under the UCL’s
 12 “unlawful” prong, Plaintiffs allege that Illuminate violated a number of statutes, and
 13 thus have adequately alleged violation under the unlawful prong. ¶ 275.

14 Similarly, Plaintiffs can demonstrate violations of the UCL under the “unfair”
 15 prong, that “creates a cause of action for a business practice that is unfair even if not
 16 proscribed by some other law.” *In re Adobe Sys.*, 66 F. Supp. 3d at 1226; *Grimstad v.*
 17 *FCA US, LLC*, 2018 WL 6265087, at *9 (C.D. Cal. May 24, 2018) (“Because
 18 Plaintiffs have specifically alleged the conduct they claim is ‘immoral, unethical,
 19 oppressive, fraudulent and unscrupulous,’ the Court finds that Plaintiffs have
 20 adequately alleged an unfairness prong claim under the balancing set.”) Just as other
 21 Plaintiffs in the data breach context have, Plaintiffs can proceed under either the
 22 balancing or tethering tests Courts used to evaluate claims under the “unfair” prong
 23 because on balance, the gravity of Illuminate’s violations of childrens’ privacy rights
 24 vastly outweighs the utility of its conduct and because Plaintiffs have identified a
 25 number of important public policy considerations and statutes that Illuminate has
 26 violated. *Id.* at 1226-28. The UCL is the means by which Plaintiffs seek to enforce
 27 these rights. ¶ 275 (“Defendant has engaged in unfair competition within the meaning
 28 of California Business & Professions Code section 17200, *et seq.*”).

1 Likewise, Plaintiffs' NY General Business Law ("NY GBL") and Colorado
 2 Consumer Protection Act ("CO CPA") claims also succeed because no reliance is
 3 required. "[A] private action brought under § 349 does not require proof of actual
 4 reliance[.]" as Plaintiffs only need to draw an adequate casual connection between
 5 the deceptive trade practices and their injuries.¹² *Pelman ex rel. Pelman v.*
 6 *McDonald's Corp.*, 396 F.3d 508, 511 (2d Cir. 2005) (citations omitted); *see also*
 7 *Griffey v. Magellan Health Inc.*, 2022 WL 1811165, at *8-9 (D. Ariz. June 2, 2022)
 8 (allowing NY GBL § 349 data breach claim without allegations of actual reliance);
 9 *In re Blackbaud*, 2021 WL 3568394 at *12-14 (same).

10 Similarly, "in order to state a [CO] CPA claim, a plaintiff must allege as one
 11 of the elements that he suffered injury in fact to a legally protected interest and that
 12 the defendant's actions in violation of the [CO] CPA were the cause of the plaintiff's
 13 injury."¹³ *US Fax L. Ctr., Inc. v. iHire, Inc.*, 374 F. Supp. 2d 924, 929 (D. Colo.
 14 2005), *aff'd*, 476 F.3d 1112 (10th Cir. 2007). Here, as stated above, Plaintiffs pleaded
 15 that Illuminate failed to safeguard their PI/PHI and comply with various laws and
 16 regulations, which caused unauthorized disclosure of their PII/PHI. *See supra*
 17 Section I; *see e.g.* ¶¶ 45, 101-109. This unauthorized disclosure resulted in loss of
 18 time, diminution of the value of PI/PHI, increased spam communications, hacked
 19 accounts, and emotional distress. *See id.*; *see also Gaston v. FabFitFun, Inc.*,
 20 2021 WL 3362028, at *1 (C.D. Cal. Apr. 2, 2021) (preliminarily approving class
 21 settlement of CO CPA claims arising from data breach).

22
 23
 24
 25
 26 ¹² Defendant only challenges the causation element of the GBL (MTD at 24-25), and
 27 thus concedes that the act or practice is "consumer oriented." *See In re Blackbaud*,
 2021 WL 3568394, at *12 (D.S.C. Aug. 12, 2021).

28 ¹³ Again, Defendant only challenges the causation element of the CO CPA, and thus
 concedes that all other elements are satisfied. MTD at 24-25.

B. Plaintiffs Have Adequately Pleaded Their California Consumer Privacy Act (“CCPA”) and California Confidentiality of Medical Information Act (“CMIA”) Claims¹⁴

1. CCPA

Defendant argues that there is no private right of action available to Plaintiffs under the CCPA because it is a “service provider” and not a “business.” MTD at 26. However, because Illuminate “could be both a ‘service provider’ and a ‘business’ under the CCPA, it would not be insulated from liability under the CCPA if it qualified as a ‘service provider.’” *In re Blackbaud*, 2021 WL 3568394, at *6; *Karter v. Epiq Sys., Inc.*, 2021 WL 4353274, at *2 (C.D. Cal. July 16, 2021) (discussing that although a class action administrator services class members, it is a business because it collects consumers’ personal information). The CCPA defines a “business” as a for-profit entity (1) “that is organized or operated for the profit or financial benefit of its shareholders or other owners that collects consumers’ personal information[;] or” (2) “on the behalf of which that information is collected[;] or” (3) “that alone, or jointly with others, determines the purposes and means of the processing of consumers’ personal information[.]”¹⁵ Cal. Civ. Code § 1798.140(c).

Here, Plaintiffs plausibly allege that Illuminate “alone, or jointly with others, determines the purposes and means of the processing of consumers’ personal information.” *Karter*, 2021 WL 4353274, at *2 (citing Cal. Civ. Code § 1798.140(c)(1)). Specifically, Plaintiffs allege that Illuminate collects among other things, students’ attendance and grades, names, birth dates, class schedules, behavioral records, and health and socio-economic information such as whether they qualify for special education or free or reduced-price lunches. ¶ 5. Illuminate and

¹⁴ Plaintiffs submit that they are “customers” under the CRA, but acknowledge that this Court has previously rejected the application of that statutory definition to similar claims but nonetheless raise the claim to preserve the record and for potential appeal. *Patton v. Experian Data Corp.*, 2018 WL 6190349, at *8 (C.D. Cal. Jan. 23, 2018).

¹⁵ Plaintiff also alleges that Illuminate services 17 million students, meaning that it receives the personal information of well over 50,000 or more consumers, thus meeting other requirements under the CCPA. ¶ 2.

educators using its platforms then use this information to determine whether interventions and assessments are effective and whether further steps, plans, or actions are necessary. It is also plausible that Illuminate processes this information to further develop its many platforms. ¶ 4. Thus, “[a]t this early stage, Plaintiff has plausibly alleged that Defendants may be held liable as a business under the CCPA.” **Error! Bookmark not defined.***Karter*, 2021 WL 4353274, at *2.

2. CMIA

Illuminate argues that it is not a “provider of health care” under CMIA because it is not in the medical business. MTD at 27. However, “[i]n amending Cal. Civ. Code § 56.06 to include businesses that maintain or offer software that maintains medical information, the California legislature intended to ensure that the CMIA would apply to all businesses that maintain medical information whether or not the business was organized for that purpose.” *In re Blackbaud*, 2021 WL 3568394, at *8 (quotation marks and citations omitted); *see Stasi*, 501 F. Supp. 3d at 911 (“the plain language of the statute demonstrates that, in the California legislature’s judgment, the provisions of CMIA at issue here are substantive, not procedural.”) (citations omitted). Instead, a business can qualify as a “provider of health care” if it offers software or hardware to consumers (1) “in order to make the information available to an individual or a provider of health care at the request of the individual or a provider of health care,” (2) “for purposes of allowing the individual to manage his or her information, or” (3) “for the diagnosis, treatment, or management of a medical condition of the individual[.]” *Id.*

Here, Plaintiffs plausibly allege that Illuminate offered its software for such uses. Like the Plaintiffs in *In re Blackbaud*, they claim that “Illuminate’s systems were designed, in part, to make medical information available to schools by providing cloud-based computing solutions through which the schools could store, access, and manage current and former students’ medical information that are part of their school records.” ¶ 298; *In re Blackbaud*, 2021 WL 3568394, at *7-8. Plaintiffs also allege

1 that Illuminate and educators on Illuminate platforms use this information to identify
 2 student needs and ways to manage them. ¶¶ 1, 4-5. Thus, it is plausible that
 3 Illuminate’s software was used in their education and allowed families and their
 4 educators to “to manage his or her information” and that data is used “for the
 5 diagnosis, treatment, or management of [Plaintiffs’] medical condition[s.]” Cal. Civ.
 6 Code § 56.06(b). For example, a parent may use their child’s educational and
 7 behavioral records to diagnose or treat any number of learning or behavioral
 8 disorders, or even a food allergy. *See Corona v. Sony Pictures Ent., Inc.*, 2015 WL
 9 3916744, at *8 (C.D. Cal. June 15, 2015) (finding that disclosed information
 10 regarding details of an employee’s child with special needs was protected health
 11 information). “Accordingly, California Plaintiffs plausibly allege that [Illuminate]
 12 constitutes a ‘provider of health care’ under Cal. Civ. Code § 56.06(b).” *In re*
 13 *Blackbaud*, 2021 WL 3568394, at *8.

14 Finally, Illuminate argues that “‘disclosure’ under the CMIA requires an
 15 *affirmative* act by the defendant.” MTD at 28 (emphasis in original). Defendant is
 16 wrong. “The CMIA *does not require an affirmative act* of communication by the
 17 Defendant...The plain text of the statute does not require an affirmative disclosure
 18 by the medical provider to create liability but in fact creates a remedy for those who
 19 store records negligently.” *In re Solara*, 2020 WL 2214152, at *7 (emphasis added).
 20 Illuminate’s one authority in support is distinguishable. There, the court held that
 21 “[n]o breach of confidentiality takes place until an unauthorized person views the
 22 medical information.” *Sutter Health*, 227 Cal. App. 4th at 1557. Here, like *In re*
 23 *Solara*, Plaintiffs have alleged that they received letters stating that their information
 24 may have been compromised, and that they have had an increase in spam following
 25 the Breach. *In re Solara*, 2020 WL 2214152, at *7 (holding “[t]hese events plausibly
 26 give rise to the inference that Plaintiffs’ information was exposed in the Breach”).
 27 Thus, California courts that have had occasion to consider Defendant’s argument
 28

1 have rejected it. *Id.* (citing *Regents of Univ. of Cal. v. Superior Court*, 220 Cal. App.
2 4th 549, 568 (2013)).

3 **C. Plaintiffs Have A Right Of Action Under The Colorado Security**
4 **Breach Notification Act**

5 Under Colo. Rev. Stat. § 6-1-716(2), entities that maintain, own, or license
6 data that includes personal information about a resident of Colorado must comply
7 with notification requirements. Illuminate does not dispute that it maintains, owns,
8 or licenses data that includes personal information about Colorado residents, but
9 instead argues that the statute does not create a private right of action. MTD at 30.
10 However, Colorado’s data-breach notice statute provides that the “attorney general
11 may bring an action ... to address violations of this section,” but also provides that
12 the “provisions of this section are not exclusive.” Colo. Rev. Stat. § 6-1-716(4).
13 Courts have reasoned that this permissive language is “at least ambiguous as to
14 whether there is a private right of action” and concluded that, “absent any authority
15 construing this ambiguity to exclude private rights of action,” the claims should not
16 be dismissed.¹⁶ *In re Equifax, Inc., Customer Data Sec. Breach Litig.*, 362 F. Supp.
17 3d 1295, 1341 (N.D. Ga. 2019) (quoting *In re Target Corp. Data Sec. Breach Litig.*,
18 66 F. Supp. 3d 1154, 1169 (D. Minn. 2014)).

19 **VIII. PLAINTIFFS’ REQUEST FOR DECLARATORY RELIEF IS NOT**
20 **DUPLICATIVE**

21 Contrary to Defendant’s contention, the request for declaratory judgment is
22 not duplicative of relief sought under another cause of action. Fed. R. Civ. P. 57
23 (“The existence of another adequate remedy does not preclude a declaratory
24 judgment that is otherwise appropriate.”). Here, absent an injunction, Illuminate is
25 likely to continue to violate state and federal law regarding consumer data
26

27 ¹⁶Even Defendant’s own authority did not find the statutory language determinative
28 of dismissal. *See Engl v. Nat. Grocers by Vitamin Cottage, Inc.*, 2016 WL 8578096,
at *12 n.9 (D. Colo. June 20, 2016).

1 protections. Defendant does not agree that it has committed such violations.
 2 Therefore, an actual controversy exists. Plaintiffs seek a judicial determination of
 3 whether Defendant has performed, and is performing, its statutory and contractual
 4 privacy obligations that are necessary to protect and safeguard Plaintiffs' PI/PHI and
 5 others' sensitive data from further unauthorized, access, use, and disclosure, or
 6 insecure disposal. Such a determination would immediately reduce the likelihood of
 7 continuing and future harm to Plaintiffs and other similarly situated.

8 Defendant's citation to *Mangindin v. Wash. Mut. Bank*, 637 F. Supp. 2d 700,
 9 707-708 (N.D. Cal. 2009) is, at best, misleading. The *Mangindin* found "that the
 10 declaratory relief Plaintiffs seek is *entirely commensurate* [not substantially similar
 11 to] with the relief sought through their other causes of action." *Id.* (emphasis added).
 12 In the present matter, the aim of immediately reducing the likelihood of continuing
 13 and future harm to Plaintiffs is not entirely commensurate with the other pled causes
 14 of action. Even this interpretation of *Mangindin* runs afoul of the language of the
 15 Declaratory Judgment Act which indicates that declaratory judgment is available
 16 "whether or not further relief is or could be sought [emphasis added]." 28 U.S.C. § 2201.
 17

18 CONCLUSION

19 For the above reasons, Plaintiffs ask that the Court deny Defendant's MTD.
 20 Should the Court grant it in any respect, Plaintiffs ask for leave to amend. *Socal*
 21 *Recovery, LLC v. City of Costa Mesa*, 2019 WL 1090774, at *1 (C.D. Cal. Jan. 29,
 22 2019) ("it is an abuse of discretion for a district court to refuse to grant leave to amend
 23 a complaint").

24 Respectfully submitted,

25 **KAPLAN FOX & KILSHEIMER LLP**

26 DATED: February 21, 2023

27 By: /s/ Laurence D. King
 28 Laurence D. King

Laurence D. King (SBN 206423)
Matthew B. George (SBN 239322)
Blair E. Reed (SBN 316791)
1999 Harrison Street, Suite 1560
Oakland, CA 94612
Telephone: 415-772-4700
Email: *lking@kaplanfox.com*
mgeorge@kaplanfox.com
breed@kaplanfox.com

KAPLAN FOX & KILSHEIMER LLP
Joel B. Strauss (admitted *pro hac vice*)
850 Third Avenue, 14th Floor
New York, NY 10022
Telephone: 212-687-1980
Email: *jstrauss@kaplanfox.com*

KAPLAN FOX & KILSHEIMER LLP
Justin B. Farar (SBN 211556)
12400 Wilshire Boulevard, Suite 460
Los Angeles, CA 90025
Telephone: 310-614-7260
Email: *jfarar@kaplanfox.com*

Plaintiffs' Co-Lead Interim Counsel

**KANTROWITZ, GOLDHAMER &
GRAIFMAN, P.C.**

DATED: February 21, 2023

By: /s/ Melissa R. Emert
Melissa R. Emert

Melissa R. Emert (admitted *pro hac vice*)
Gary S. Graifman (admitted *pro hac vice*)
135 Chestnut Ridge Road, Suite 200
Montvale, NJ 07645
Telephone: 201-391-7000
Email: *memert@kgglaw.com*
ggraifman@kgglaw.com

Plaintiffs' Co-Lead Interim Counsel

HELD AND HINES LLP
Marc J. Held (admitted *pro hac vice*)
Philip M. Hines (admitted *pro hac vice*)
2044 Ralph Avenue
Brooklyn, NJ 11234
Telephone: 718-531-9700
Email: *mheld@heldhines.com*
phines@heldhines.com

SHEEHAN AND ASSOCIATES, P.C.
Spencer Sheehan (admitted *pro hac vice*)
60 Cuttermill Road, Suite 409
Great Neck, NY 11021

1 Telephone: 516-268-7080
2 Email: spencer@spencersheehan.com

3 **SHEEHAN AND ASSOCIATES, P.C.**
4 Theodore Hillebrand
5 65-24 78th Street
6 Middle Village, NY 11379
7 Telephone: 929-246-0747
8 Email: thillebrand@spencersheehan.com

9 *Plaintiffs' Executive Committee*

10 *Attorneys for Plaintiffs and the Proposed*
11 *Class*

ATTESTATION PURSUANT TO CIVIL L.R. 5-4.3.4(a)(2)

I hereby attest that the other signatory listed above, and on whose behalf this filing is submitted, concurred in the filing's content and has authorized the filing.

/s/ Laurence D. King
Laurence D. King

CERTIFICATE OF SERVICE

I hereby certify that on February 21, 2023, I caused the foregoing document to be electronically filed with the Clerk of the Court by using the CM/ECF system, which will automatically send an email notification of such filing to the attorneys of record who are registered CM/ECF users.

/s/ Laurence D. King
Laurence D. King